

Contents

1. New SUPREMA Biometric Reader Support.....	2
2. Virtual Dongle Support	2
3. NSL TDT Support.....	3
4. Sending SMS Upon Event	3
5. Cardholder Management Enhancement.....	3
<i>5.1. Cardholder screen is now customizable</i>	<i>3</i>
<i>5.2. Each Department can have its own default Access Group(s).....</i>	<i>4</i>
<i>5.3. 'Global Change' on Access Groups can be made on Search results</i>	<i>5</i>
<i>5.4. Card enrolment may be restricted to an enrolment reader.....</i>	<i>5</i>
<i>5.5. Option for keeping badges replaced by an Import as 'free' badges</i>	<i>6</i>
6. New Specific Log Entries for Transactions with 'Stolen', 'Lost' and 'Cancelled' Badges	6
7. New Formats for USB Readers.....	7
8. Displaying the Picture of the Escort.....	7
9. New DVRs Added	8
<i>9.1 DVTEL.....</i>	<i>8</i>
<i>9.2 NICE</i>	<i>8</i>
<i>9.3 Dedicated Micros</i>	<i>9</i>
<i>9.4 HIKVision</i>	<i>9</i>
<i>9.5 Viewer Path option.....</i>	<i>10</i>
<i>9.6 Generic DVR.....</i>	<i>10</i>
10. Alarm Enhancements	10
11. Reports	11
<i>11.1 Statistics.....</i>	<i>11</i>
<i>11.2 Transaction codes</i>	<i>11</i>
<i>11.3 Last X hour field</i>	<i>12</i>
<i>11.4 Additional audit information when creating/removing group of cards/cardholders.....</i>	<i>12</i>
12. Multi-Site Improvements	13
13. Software Optimizations	13
<i>13.1 User passwords can be required to have a minimum number of characters</i>	<i>13</i>
<i>13.2 New Search option has been added to screens that can have long lists</i>	<i>14</i>
<i>13.3 Dongle cardholder limitation takes into account only cardholders who have a badge.....</i>	<i>14</i>
<i>13.4 The # key after the PIN code can now be controlled by Amadeus 5.....</i>	<i>15</i>
<i>13.5 Changes in the automatic cleaning of the event log.....</i>	<i>16</i>
<i>13.6 Redundant Server supports Centralized Spread</i>	<i>16</i>
14. Integrations.....	17
<i>14.1 KEEISING.....</i>	<i>17</i>
<i>14.2 Updated XML-API.....</i>	<i>18</i>
<i>14.3 Updated OPC server.....</i>	<i>18</i>
15. Communication	18
<i>15.1 Support for communication with controllers over Internet.....</i>	<i>18</i>
<i>15.2 Controller communication has been optimized</i>	<i>18</i>
16. Tools	20
<i>16.1 New DDS Maintenance tool for SQL databases.....</i>	<i>20</i>
<i>16.2 Log Archiving Support</i>	<i>20</i>
<i>16.3 New DDS tool for converting database from MDB to SQL.....</i>	<i>21</i>
<i>16.4 Automatic tool for deleting old visitors</i>	<i>21</i>
17. New Help & New Amadeus 5 User Manual.....	21
18. Additional Language	22
19. MS/SQL2008	22

1. New SUPREMA Biometric Reader Support

Two new Suprema Biometric Readers have been integrated into the Amadeus 5 system:

- BioLiteNet - Finger/Card/Keypad/Display
- BioEntryPlus – Finger/Card

EM Marine and Mifare cards are supported, following to the reader type:

Reader Type	EM Marine	Mifare
BioEntry Plus	BEP	BEPM-OC
BioLite Net	BLR-OC	BLN-OC

As the other DDS biometric readers, the same functions are available in Amadeus 5 (enrolment, downloading, etc.)



- Only '**Finger only**' and '**Card+Finger**' modes are supported
- Automatic badge creation after enrollement
- TCP or serial RS485 protocol
- Administrator password

The reader configuration has to be done from the [Suprema software](#) (BioStar)

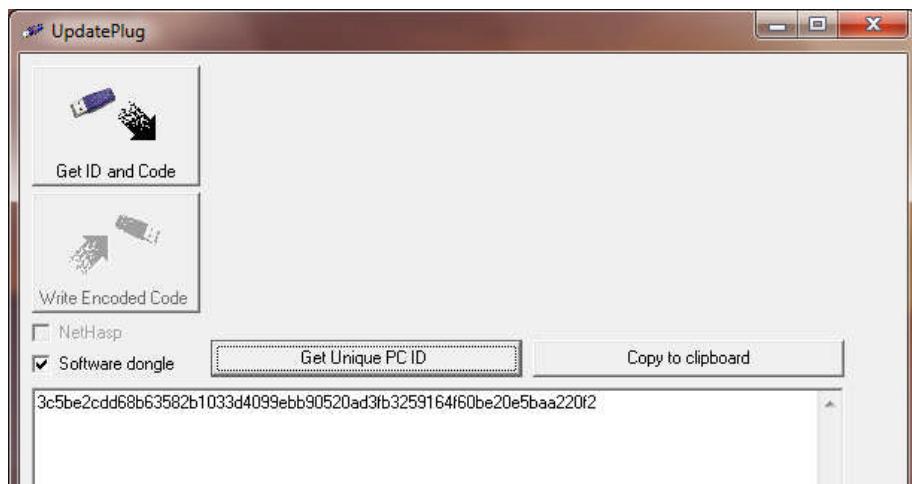
These readers require the ini option: **Suprema=1**.

The ini option **BioCreateBadge=1** enables the automatic badge creation during enrollement.

Note that it is no more possible to allocate to controllers and biometric readers the same network. We had already warned in the past not to make this connection. Now, we have decided to completely restrict this possibility in Amadeus 5 in order to avoid future communication problems.

2. Virtual Dongle Support

The virtual Dongle is now the standard way for the Amadeus 5 license to be distributed. In order for us to supply a license we must know the **Unique PC ID** of the target end user machine, in addition to the required configuration (total no. of cardholders/workstations, alarm & graphic modules, etc.). The **Unique PC ID** is given by our **UpdatePlug** utility located on the application folder. Running the UpdatePlug.exe file, selecting 'Software Dongle' and clicking on '**Get Unique PC ID**' would give the following:



The **Unique PC ID** should be copied and sent to us by email. Once we get it, we send the 2 license files based on the ordered configuration. These files are: **Data.plg** and **Signature.plg**.

Once received, they must be copied into the server application folder.

It is required to set **Software Dongle = 1** in INI file.

Note: Physical USB dongles are still supported and can still be ordered.

3. NSL TDT Support

Amadeus 5 now supports NSL TDT (Ticket Dispenser Terminal) controller (belongs to the NSL family), which in addition to its standard security features, is able to print programmable tickets on a serial printer for ticket printing applications (e.g. cafeteria meal tickets).

For sending the cardholder names to the NSL TDT, a new option has been added in the controller screen, “**Send Cardholder Names**”. This option, available when selecting the controller type ‘OPEN/NSL4’, allows to store in the controller memory, the concatenation of the 11th first characters of the last name and first name with a space between them.

Note that after a controller is set to 'Send Cardholder Names', Amadeus 5 server and workstations must be restarted.

In the INI file, the option **NslTdtAddToAscii** allows to control ASCII code.

In addition, specific commands for coupon definition can be configured by commands in Script tab in controller screen. Please contact us for defining these commands.

This feature is supported only for SQL database.

4. Sending SMS Upon Event

Since www.smsmail.com allows to send SMS by email, Amadeus 5 can use its action for sending an email to send SMS also, after registration to this website.

For example, if you want to receive an SMS when an alarm occurs, create a ‘Send Email’ action with a short message and specify in the field ‘To’ the phone number that should receive the SMS and add “@smsmail.com” (e.g. 33612345678@smsmail.com). Then, create the associated process and the global reflex that will trigger this process upon alarm event. Note that this feature requires to fill the Email parameters in the Options screen.

5. Cardholder Management Enhancement

5.1. Cardholder screen is now customizable

- **Field captions, additional cardholder types and mandatory fields**

These changes are effective after editing the file ‘**CardholderCustom1.xml**’ located in the Application directory and changing its filename to ‘**CardholderCustom.xml**’.

Note: instructions are included in this file.

- **Bringing fields from other tabs in the General tab**

Some fields of lower-level tabs can be shown at the bottom of the main Cardholders screen, in a scrollable window, in order to regroup all the needed fields in the same screen. Note: ‘ID’ field is positioned under the ‘Number’ field.

The section **[Personalize Cardholder Screen]** in the ini file shows the categories that can be displayed. Entries are in the form:

‘**Cardholder_<info>_Move_To_General=n**’, where **<info>** defines the field

information to move, and **n** (between 1-7) defines the sequence in which they will be displayed. If **n=0**, the field is not moved.

Example: Cardholder_Address_Move_To_General = 1

Cardholder_Visitor_Move_To_General = 2

Note: for opening automatically the Cardholder screen with the maximal size, use the new INI option '**Cardholder_Open_Maximize**'.

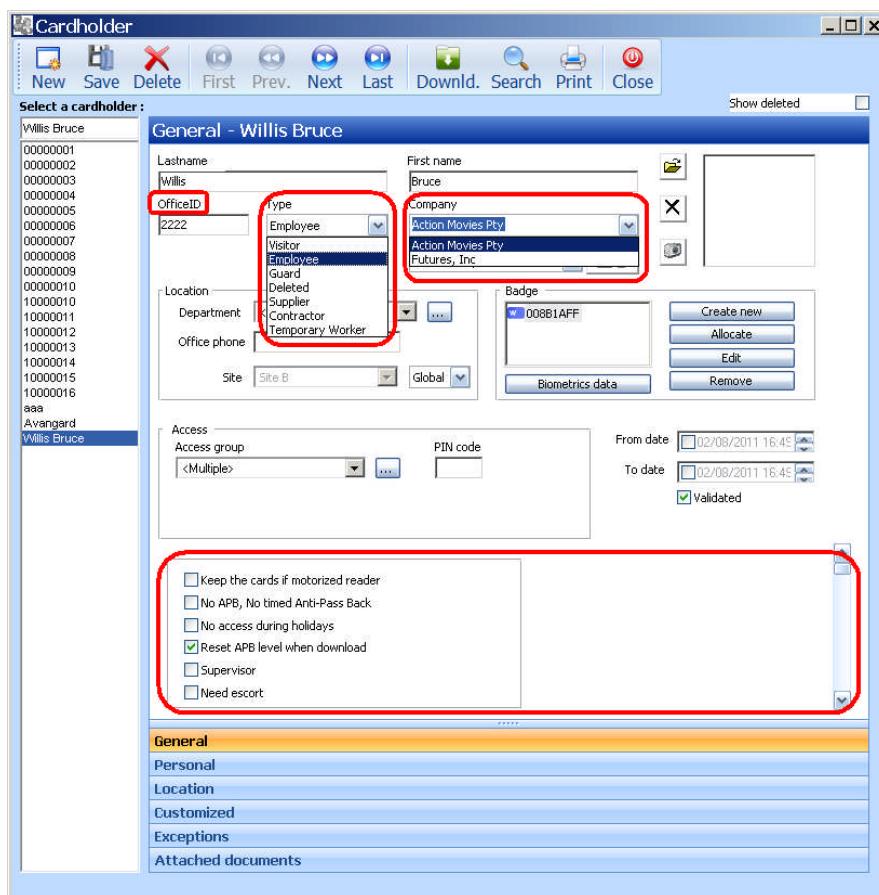
- **Company field can be shown as a Combo box**

To change the Company field into combo box, set the INI option

'Cardholder_Company_As_A_Combo=1'.

Note that it is not supported in Light version.

Here is an example of Cardholder screen customization:

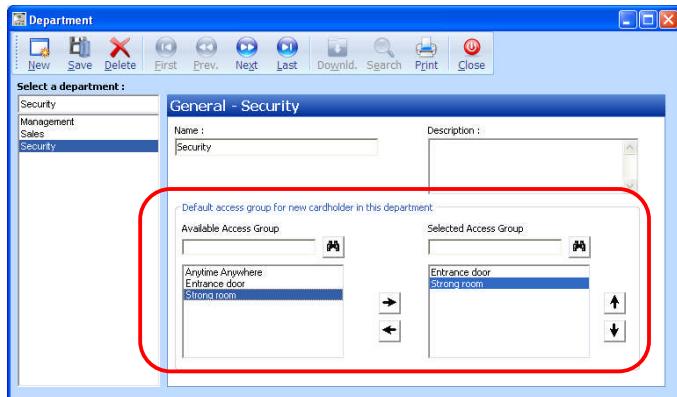


This example shows the fieldname '**Number**' changed to '**OfficeID**', additional values for the '**Type**' field, '**Company**' shown as a combo box, and Cardholder Privileges from the '**Personal**' tab shown as a scrollable box in the main Cardholder screen.

5.2. Each Department can have its own default Access Group(s)

Upon creating a new cardholder, Amadeus 5 allocates automatically the Access Group(s) according to the selected Department. This can be possible by setting the new ini entry **DepartmentAG=1** (set by default), which adds new fields to the Department screen.

These fields allow to define the default Access Groups of each Department.



For example, each member of the Security Department must belong to the Access Groups 'Entrance door' and 'Strong room'. After adding these Access Groups to the Security Department as in the above picture, every new cardholder of the Security Department will belong to these Access Groups automatically.

Notes:

- This feature is not available when using simple access groups (when the INI entries "MultiSite=0" and "ForceMultipleAG=0").
- This feature is stronger than the INI entries '**VisitorDefaultAccessGroup**' and '**CardholderDefaultAccessGroup**'.
- This feature is stronger than the option '**Also for Visitor screen**' in the Access Group screen.

5.3. 'Global Change' on Access Groups can be made on Search results

Let's say that a new reader has been installed and a part of the cardholders (for example, a whole department, a specific company, etc.) should have access to it.

Adding this reader to each Access Group may be a fastidious work and could not be a good solution if Access Groups are shared with people who do not have access to that reader. Create an Access Group with this reader only is a good solution but how to add this Access Group to the right people?

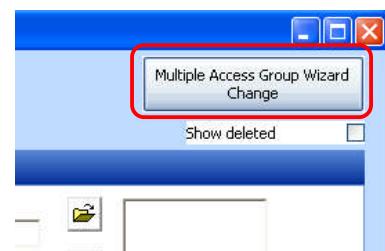
Adding access groups to a part of cardholders in one go is now possible.

After searching people in the Cardholder screen with the Search function (e.g. for searching all people belonging to the same department, press the Search button, select the Department and press Search again), new button

"Multiple Access Group Wizard Change" is displayed at the top right corner of the screen. This button allows to add/change/remove the multiple access groups of the selected people of the search results via the Multiple Access Group Wizard.

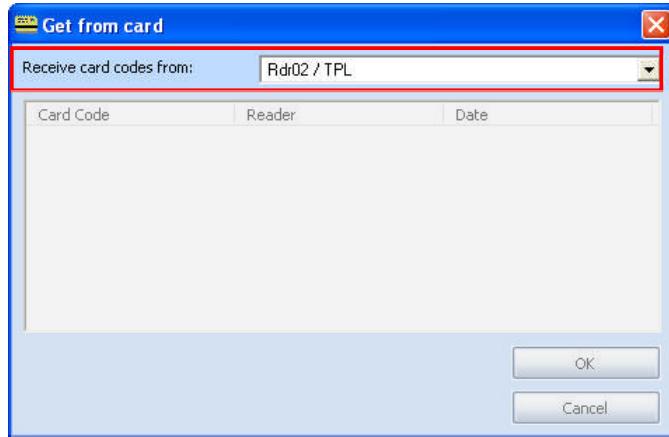
The advantage of this feature from the Tools>Multiple Access Group Wizard is that there is no need that people to be modified have a common Access Group.

Note that the changes can be performed for cardholders having 'multiple' access groups only.



5.4. Card enrolment may be restricted to an enrolment reader

The new added list of 'Get from card' screen allows filtering cards enrolment on a single enrolment reader.



Note that at the opening of the screen, Amadeus 5 remembers the last selection.

5.5. Option for keeping badges replaced by an Import as 'free' badges

When someone has to change his card for any reason, it may be useful to keep his old card in the system as 'free' card. In the previous versions, when updating existing cardholders with new card via the Import function, the replaced cards were automatically removed from the database. Now, it is possible to choose if wanting to keep the old allocated cards as 'free' cards. By setting the new INI entry

'KeepUnallocatedBadgeAfterImport = 1', the cards replaced by the Import function are still stored in the database as 'Unallocated Badge'.

6. New Specific Log Entries for Transactions with 'Stolen', 'Lost' and 'Cancelled' Badges

For high-security sites, in order to identify immediately stolen, cancelled or lost badges in the log screen, the log event transaction for such a card is more detailed and the text color of such a transaction is customizable via the 3 following new INI entries:

Color_DeniedCancel = x (=2 by default)

Color_DeniedLost = y (=2 by default)

Color_DeniedStolen = z (=2 by default), where 'x, y, z' are the desired color value.

11/09/11 15:03:54 Access Granted 'Parson Steve' From reader 'Entrance' Transaction code 11
11/09/11 15:03:54 Access Granted 'Lewis John' From reader 'Entrance' Transaction code 10
11/09/11 15:03:58 Access Denied 'Smith Susan' From reader 'Lift <Reader not defined> 3' - Stolen
11/09/11 15:04:12 Access Granted 'Tyson Carl' From reader 'Entrance' Transaction code 10
11/09/11 15:04:12 Access Granted 'Black Jamie' From reader 'Entrance' Transaction code 11
11/09/11 15:04:12 Access Granted 'Green Lyn' From reader 'Entrance' Transaction code 10
11/09/11 15:04:25 Access Denied 'Brown Peter' From reader 'Lift <Reader not defined> 3' - Cancelled
11/09/11 15:04:12 Access Granted 'Jones Sue' From reader 'Entrance' Transaction code 11
11/09/11 15:04:12 Access Granted 'Lee Robert' From reader 'Entrance' Transaction code 10
11/09/11 15:04:16 Access Denied 'Robinson Willy' From reader 'Lift <Reader not defined> 3' - Lost

Available color values:

0 - Light Pink; 1 - Black; 2 - Red; 3 - Blue; 4 - Bordeaux; 5 - Green; 6 - Orange; 7 - Pink; 8 - Purple; 9 - Light Gray; 10 - Light Blue

In addition, these new denied reasons may be used in global reflexes as triggers; for example when a stolen card is presented at one reader, a popup message can alert the guard. Moreover, these denied reasons can be filtered in Door pass reports.

7. New Formats for USB Readers

Since Amadeus 5 v1.8.022, the Badge>Get From Card screen supports receiving card code from Paxton USB reader connected to the Amadeus 5 PC. The card format is according to the following value of the 'USBReaderFormat' entry in the INI:

USBReaderFormat = 0 (Hex)

USBReaderFormat = 1 (16 bit Decimal)

USBReaderFormat = 3 (24 bit decimal)

In addition, this new Amadeus 5 version supports for more USB readers. In fact, any USB reader that transmits the code 'as is'. The 'USBReaderFormat' entry serves to position the card code as described below:

USBReaderFormat = 0 (Save the 8 MSB digits)

USBReaderFormat = 108 (Save only 8 LSB digits)

USBReaderFormat = 109 (Save only 9 LSB digits)

USBReaderFormat = 110 (Save only 10 LSB digits)

USBReaderFormat = 111 (Save only 11 LSB digits)

USBReaderFormat = 112 (Save only 12 LSB digits)

Example: For a card that its actual 10 digits code is 1234567890,

-with USBReaderFormat = 0 the 'Get From Card' screen will show the code 12345678

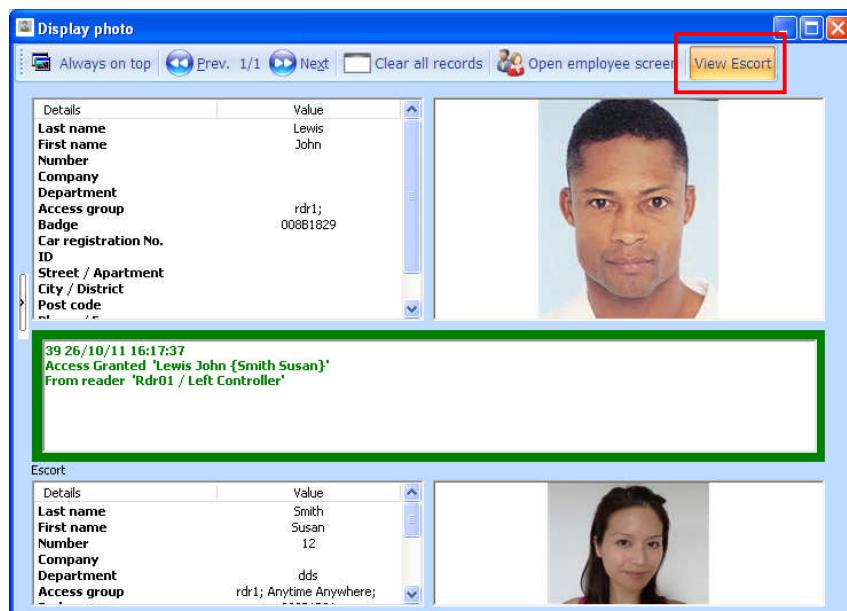
-with USBReaderFormat = 108 it will be 34567890

-with USBReaderFormat = 109 it will be 234567890.

These readers require the ini option: **UseUSBReader =1**.

8. Displaying the Picture of the Escort

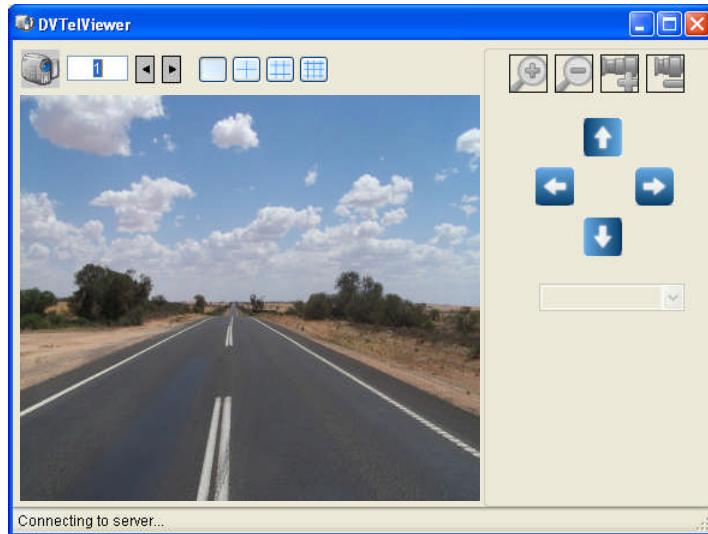
New 'View Escort' button of the Display Photo toolbar allows to display the photo of the escort also, in the case where the escort function is set. Note that the photo of the escort is slightly smaller than the photo of the main cardholder.



9. New DVRs Added

9.1 DVTEL

The DVTEL Network Video Management System software, Latitude version 6.0.0.56, has been integrated with Amadeus 5, which supports now all the cameras supported by Latitude version 6 software. Like the other DVRs already integrated, the integration consists on a viewer that can be launched from within Amadeus 5, providing live picture of a selected camera or viewing of a recorded event related to a system alarm.



Download the viewer setup at: www.dds-security.com/download/dvr/dvtel_setup.exe and install the files in any folder. The Viewer 'DvTelPlayer.exe' will be installed in the 'bin' folder. Then, set the new INI entry '**ViewerPath**' to specify the viewer location path in the hard disk.

Example: ViewerPath = C:\Program Files\Amadeus5\bin\|DvTelPlayer.exe

Note that this integration requires .Net framework 3.5 and DirectX 9.0c, which are not distributed with the setup because they are too big.

1. Microsoft .NET Framework 3.5 redistributable:

<http://www.microsoft.com/download/en/details.aspx?id=22>

2. DirectX 9.0c redistributable:

<http://www.microsoft.com/download/en/details.aspx?id=8109>

9.2 NICE

A new video viewing application, called 'alpha Mini-Viewer', has been developed by NICE for running with Amadeus 5, like the other DVRs already integrated in Amadeus 5. When running it from Amadeus 5, the alpha Mini-Viewer is connecting to the NICE alpha Engine server that should be installed previously. This server is based on the same system SDK as the NICE NVR (Network Video Recorder) software, NiceVision-FAST, allowing to support all the cameras supported by NiceVision-FAST software.

The Mini-Viewer application is launched on system start-up and has a windows task-bar icon allowing the user to open it after being minimized.

Amadeus 5 communicates with the Mini-Viewer application via a windows messages mechanism and activates the required functionalities. Once activated, the user continues operating the video using the Mini-Viewer.

The Mini-Viewer has the following functionalities:

- 1 Live video display of a selected camera

- 2 Playback of video according to an event, including 'Trick Playback' backward and forward in speeds up to x128, and frame by frame forward and backward playback
- 3 Controlling PTZ cameras including moving the camera to a pre-defined pre-set
- 4 Receiving alerts/events from the Amadeus 5 and inserting them to the FAST system as event entity - can be recorded and initiate other operations such as launching a specific video to be displayed on a wall monitor, changing video recording configuration, etc. (doesn't require a UI interaction)



Download the viewer setup at: www.dds-security.com/download/dvr/nice_setup.exe and install the files in any folder. The Viewer 'ALPHAObserver.exe' version 5.86, will be installed. Then, set the new INI entry '**ViewerPath**' to specify the viewer location path in the hard disk.

Example: ViewerPath = C:\Program Files\Nice\ALPHAObserver.exe

9.3 Dedicated Micros

In order to support the latest line of Dedicated Micros products, like **DV-IP express** and all DM range of products until January 2011, we have integrated the last NetVU.DLL version 1.7.1 of Dedicated Micros in the Amadeus 5 DM.exe viewer.

You can test it with the IP address: 212.140.243.141 (user: user, password: password) Note that this integration requires Java, not distributed with the setup. Java setup is available at: <http://www.java.com/en/download/manual.jsp>

9.4 HIKVision

Amadeus 5 supports now the NVR server software of HIKVision with the IVMS4000 client software and is compatible with the following HIKVision products:

1. Embedded encoder

2. Embedded DVR
3. Embedded Hybrid DVR
4. Embedded NVR
5. IP cameras
6. IP PTZ cameras
7. IVMS2000 software

9.5 Viewer Path option

A new INI entry '**ViewerPath**' has been added to specify the network path of the DVR viewer allowing the possibility to install the viewer in a different folder than the application folder.

Example: **ViewerPath = C:\Program Files\Avigilon\AvigilonViewer.exe**

9.6 Generic DVR

A new DVR type called '**Generic**' has been added in the DVR type list in order to let the possibility to integrate any type of DVR. Indeed, by following our specifications, anyone is able to develop external viewer for any DVR brand. The viewer should have the filename "**Viewer.exe**" and should be placed in the application folder. Then, by choosing a DVR from 'Generic' type, Amadeus 5 will use the file 'Viewer.exe' as viewer.

Note that if the value of ViewerPath is not empty then Amadeus 5 will use the given value.

Example: **ViewerPath = C:\Program Files (x86)\MyViewer\Viewer1.exe**

10. Alarm Enhancements

AlarmMsg.exe (version 1.0.05) is a small external utility to be used with Amadeus 5. It was developed mainly for hospital projects where nurses use panic buttons and it is needed to prompt a big clear message on the guard/security screen showing: who was attacked (with photo) and where.



Amadeus 5 runs this .exe file by using the Action Type 'Execute External Application' with the command: **AlarmMsg.exe /cid=%cid/rid=%rid**

For this new feature, Amadeus 5 supports the following dynamic texts:

%iid for input id,

%cid for cardholder id,

%rid for reader id.

AlarmMsg.exe runs with an INI file named 'AlarmMsg.ini' allowing customization. The files AlarmMsg.exe, AlarmMsg.ini must all be located on the Amadeus 5 folder. For more details, consult the document **'10TE513 Alarm Message.pdf'**.

11. Reports

11.1 Statistics

New reports have been added for statistical purposes. They allow to edit different sort of statistical reports like log records count per day or total of access per department or per visitor, etc.

Report wizard

Step 2/4: Select the source of the data and the check on the fields you want to see

Select the data source:

- Journal reports
 - Journal simple
 - Door pass
 - Alarm history
 - Active alarms
 - Doors Permissions
 - Audit Relay
 - Statistics**
 - Journal Simple Statistics**
 - Door Pass Statistics**
- Patrol reports
- Parameters
- Event handling
- Modules
- Other Reports

Available fields

- Date
- Day
- Hour
- Transaction**
- From
- Data
- User
- Count

Amadeus5 - Top 1000

Journal Simple Statistics

Day	Transaction	Count
19/08/2011	Access Granted	234
19/08/2011	Communication OK	2
19/08/2011	End of alarm	495
19/08/2011	Line cut	393
19/08/2011	Line short	53
19/08/2011	Polling error	2
19/08/2011	Power Down	1
19/08/2011	Power Up	2
19/08/2011	Start of Alarm	155

Amadeus5 - Top 1000

Door Pass Statistics

Department	Count
Financial	11
Management	3
Production	11
Sales	1
Training	18

11.2 Transaction codes

Transaction codes may be now displayed in 'Door Pass' reports. This is especially useful when using the T+ module.

Report wizard

Step 2/4: Select the source of the data and the check on the fields you want to see

Select the data source:

- Journal reports
 - Journal simple
 - Door pass
 - Alarm history
 - Active alarms
 - Doors Permissions
 - Audit Relay

Available fields

- Date
- Transaction
- Reader
- Name in journal
- Denied reader
- Transaction code
- Full name
- Last name
- First name

Reports preview

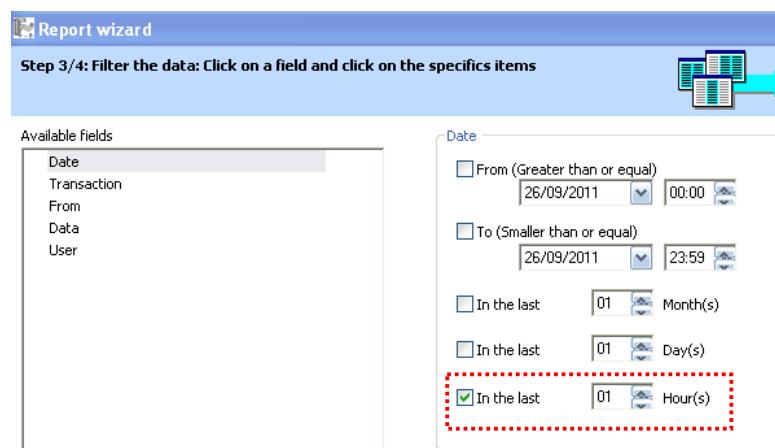
Door pass

Date	Reader	Transaction code	Full name
27/09/2011 15:43:10	Rdr01 / Controller 003	0	Robinson Willy
27/09/2011 15:43:13	Rdr01 / Controller 003	0	Brown Peter
27/09/2011 15:43:13	Rdr01 / Controller 003	0	Smith Susan
27/09/2011 15:43:52	Rdr01 / Controller 003	80	Robinson Willy
27/09/2011 15:43:56	Rdr01 / Controller 003	76	Brown Peter
27/09/2011 15:44:01	Rdr01 / Controller 003	19	Smith Susan
27/09/2011 15:44:05	Rdr01 / Controller 003	12	Brown Peter

Preview Design

11.3 Last X hour field

A new filter in the Report Wizard allows to select the events that occurred ‘in the last x hours’.



11.4 Additional audit information when creating/removing group of cards/cardholders

When using the ‘Create a Group of Badges’ screen to create or remove a group of cards/cardholders, the information of which cards/cardholders were added/removed, when, and by which user, is now available after activating the ‘New record’ and the ‘Delete record’ options in the Tools>Options>Menu screen (selecting ‘Yes’ for saving in the Journal and/or selecting ‘Yes’ for displaying in the log event screen).

Options

Menu

Message	Save	Display	Colour
Reader connected	Yes	Yes	Green
User Acknowledgment	Yes	Yes	Black
User Confirmation	Yes	Yes	Black
User Comment	Yes	Yes	Black
Unknown Card	Yes	Yes	Red
Unknown card + unsuccessful succ	Yes	Yes	Black
Non Allocated Badge	Yes	Yes	Red
New record	Yes	Yes	Blue
Save record	Yes	Yes	Blue
Delete record	Yes	Yes	Blue

For example, we can have the following records in the log screen and in the journal:
-after creating one group of 2 cards:

New record in screen 'CreateGRP (Create Cardholder)': '10000001' - User: dds
 New record in screen 'CreateGRP (Create Badge)': '10000001' - User: dds
 New record in screen 'CreateGRP (Create Cardholder)': '10000002' - User: dds
 New record in screen 'CreateGRP (Create Badge)': '10000002' - User: dds

-after removing one group of 2 cards:

Delete record in screen 'CreateGRP (Delete Cardholder)': '10000021' - User: dds
Delete record in screen 'CreateGRP (Delete Badge)': '10000021' - User: dds
Delete record in screen 'CreateGRP (Delete Cardholder)': '10000022' - User: dds
Delete record in screen 'CreateGRP (Delete Badge)': '10000022' - User: dds

In addition, when removing deleted cardholders or unallocated cards from the database from the two buttons of the screen 'Tools>Create a group of badges>Delete', the information of which cards/cardholders were removed, when, and by which user is available in the same way. Example:

Delete record in screen 'CreateGRP (Delete all non allocated badges)': '00000999' - User: dds
Delete record in screen 'CreateGRP (Remove all deleted cardholders)': '10000001' - User: dds

12. Multi-Site Improvements

- **'Global' and 'Shared' people are viewable in Reports for all the users**

Since 'Global' and 'Shared' cardholders are viewable in the Cardholders screen, these cardholders are now viewable in the reports by any user also.

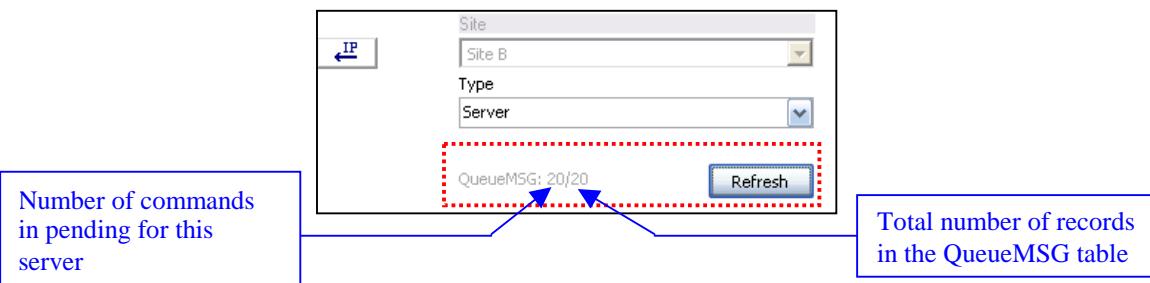
- **Customized fields are now visible in Cardholders screen for all the users**

In Multi-Site configuration, ALL the users can now see in 'Cardholders>Customized' screen, the Customized fields of 'Shared' and 'Global' cardholders of other sites.

For example, if 'Site A' has its own 'Customized fields', e.g. "Age", "Eye color", etc., in 'Cardholders>Customized' screen, users who control Site A can fill these fields for 'Local' cardholders of Site A and all 'Global' cardholders. Now, even users who don't control Site A can view "Age" and "Eye color" fields of 'Shared' and 'Global' cardholders.

- **In 'Computer' screen the total QueueMSG is displayed for each PC**

The 'QueueMSG' is the database table where the different commands between the servers are exchanged. The information of the current number of commands in pending for a server and the existing total number of records in the QueueMSG table is now displayed in the 'Computer' screen. A 'Refresh' button allows to update the information.



Note: this information is also displayed for workstations, but it is not significant.

13. Software Optimizations

13.1 User passwords can be required to have a minimum number of characters

Some companies require that user authentication password must have at least 8 characters, including numerals or special characters. For that reason, Amadeus 5 can

force now users to use minimum number of characters and minimum mixes of letters and digits for their password.

The two following ini entries allow to define rules for the user password:

PasswordMinLength = n defines minimum length for the password (=1 by default)

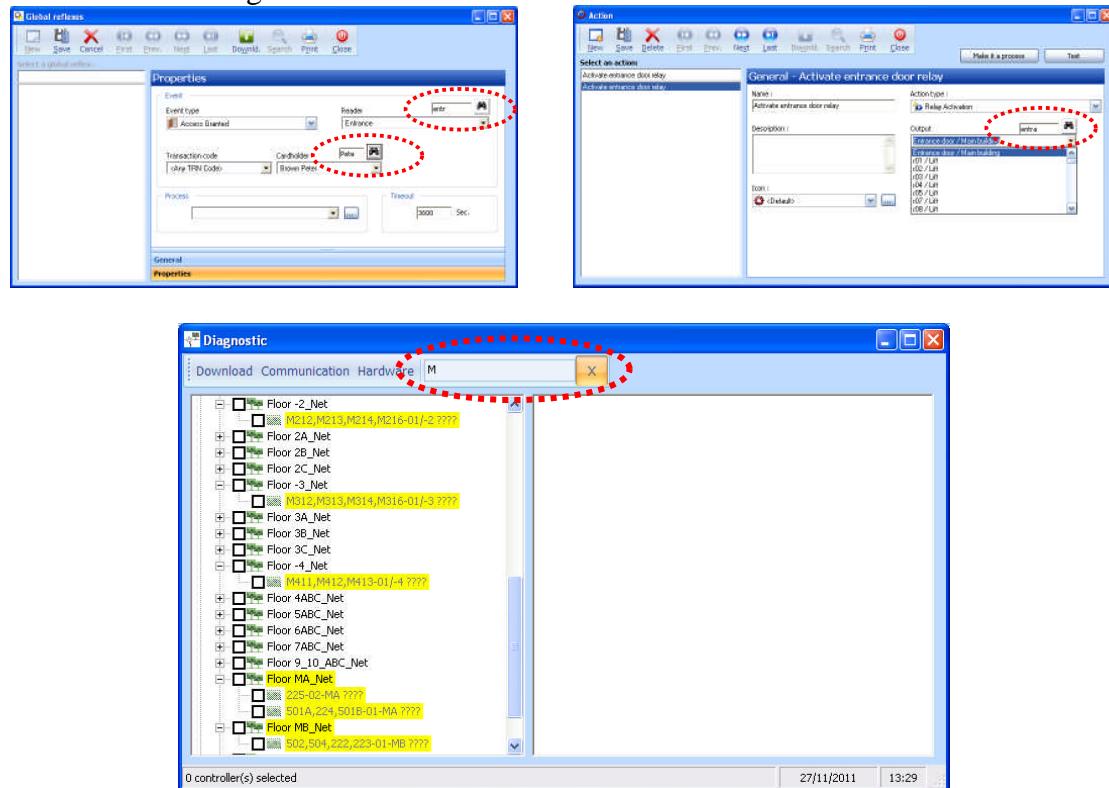
PasswordMixNumber = n defines the minimum number of letters and digits.

Example: PasswordMixNumber =2, would require at least 2 letters and 2 digits.

Note: this option does not deal with forcing lower case and upper case letters.

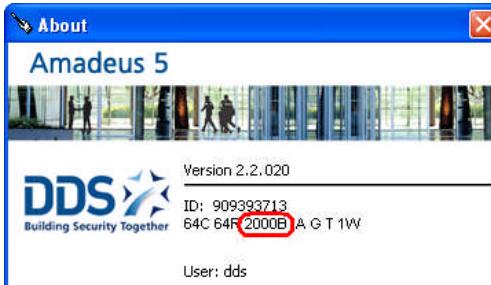
13.2 New Search option has been added to screens that can have long lists

New Search field has been added in places where it may be possible to have long lists, like reader list, input list, cardholder list in Global Reflex screen and in Action screen and controller list in Diagnose screen.



13.3 Dongle cardholder limitation takes into account only cardholders who have a badge

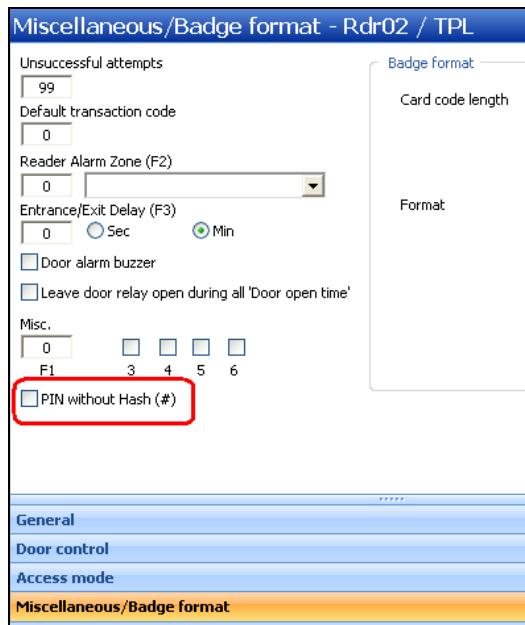
In order to generate historical reports, some sites store all their visitors in Amadeus 5, even visitors who have left the site several months ago. This method can quickly lead to reach the maximum cardholder limitation of the dongle unless using the new Amadeus 5 version.



Until now, the dongle cardholder limitation was on all the cardholders, even those that do not have a card (except deleted cardholders). From this software version, the limited number of cardholders of the dongle is relative to cardholders who have a badge only. For example, on one installation where visitors are created every day, a batch of 200 cards is dedicated for visitors. When new visitor arrives, he receives the card of an old visitor, but old visitors are not deleted from the database. After 10 days, the database contains 2,000 visitors and a dongle of 2,000 badges is not sufficient if using former versions. Now, the limit is based on cardholders who have a badge only and a dongle of 2,000 badges is sufficient in this situation, even if old cardholders/visitors are not deleted.

13.4 The # key after the PIN code can now be controlled by Amadeus 5

When using Keypad reader and accessing via PIN code, it was necessary to press the # key after PIN code. A new option "**PIN without Hash (#)**" has been added in the Reader>Miscellaneous screen allowing to avoid the need to press the Hash Key (#) after entering the PIN code (relevant when the reader is defined to check the PIN code). This option is supported on controller firmware versions 18/10/10 and later.



13.5 Changes in the automatic cleaning of the event log

In version 1.8.016, we introduced INI options to automatically clean up a part of the log text because we found that on large systems, when the real time log contains many events, the application may start to react very slow. But we just found that despite this, the log can increase indefinitely if these options are configured incorrectly.

For example, suppose that at each 1000 events (LogCleanFrequency), Amadeus 5 checks if the log has more than 4000 lines (LogMaxLines) and if yes, it removes 500 lines (LogEraseLines).

So

After 5,000 events, log will have 4,500 lines as we removed 500

After 6,000 events, log will have 5,000 lines as we removed 500 from 5,500

After 7,000 events, log will have 5,500 lines as we removed 500 from 6,000

...

After 30,000 events, log will have 17,000 lines.

To simplify, the LogEraseLines (for Rich log) and LogEraseCharacters (for Simple log) options have been removed for using only LogMaxLines and LogMaxCharacters options. Then, if the LogMaxLines (or LogMaxCharacters) is reached, all the lines are deleted from the log except the last LogMaxLines (or LogMaxCharacters).

In the above example, once the log reaches the 4000 lines limit (LogMaxLines), it stays at this number of lines.

Note: these options are set by default to always keep the latest 1000 events (approx.):

LogCleanFrequency = 100

LogMaxCharacters = 100000

LogMaxLines = 1000

13.6 Redundant Server supports Centralized Spread

Centralized spread is a way that allows multiple PCs to connect to a single Spread instance (deamon), by using a single executable 'spread.exe', thus avoiding communication difficulties between Amadeus 5 server and its workstations (due to firewalls, anti-virus, or when the remote computers are only allowed to be connected to the server but not to each other, etc.). The Centralized spread configuration is described in the document **'10TE512 Connecting multiple computers to a single Spread deamon'**.

Until now, the method of Centralized Spread was not compatible to environment of redundant servers because all the workstations lost their spread connection when the main server failed. For this reason, the two following ini options have been added:

SpreadDeamonBackup = 4803@<NAME_OF_REDUNDANT_SERVER>, which defines the 'SpreadDeamon' option of the Redundant Server.

SpreadDeamonWaitBeforeSwapSec = 60 (default), which defines the delay before swapping to the Redundant Server.

For example:

SpreadDeamonBackup = 4803@SERVER2

SpreadDeamonWaitBeforeSwapSec = 30

Then, when workstations do not succeed to connect to the Main Server Spread and if the delay before swapping to the Redundant Server is reached, the workstations try to

connect to the second server. When the Main Server is started, they try to connect to the Main Server again.

Note that the ‘Spread.conf’ file should contain both servers (and should be set like that in both servers).

Example:

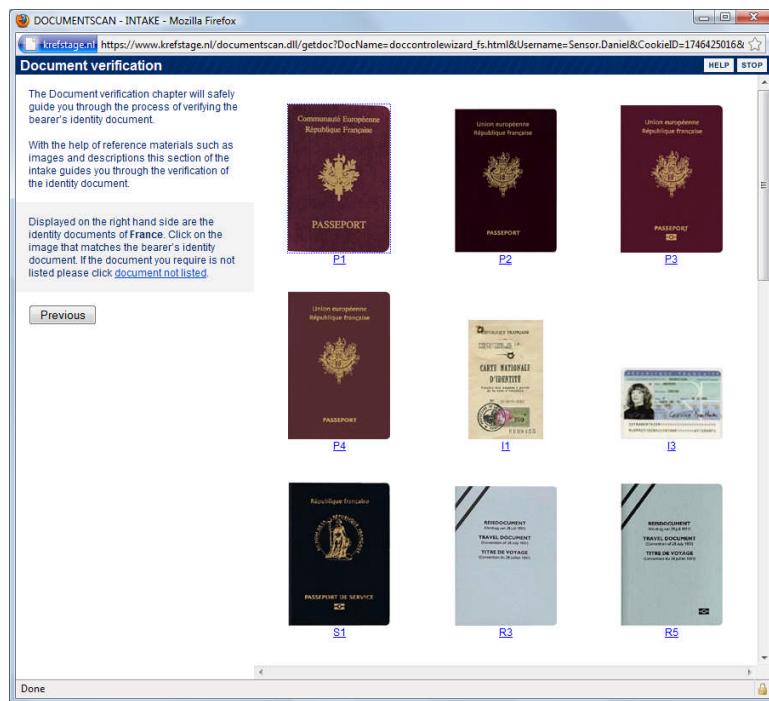
```
Spread_Segment 239.0.0.60:4803 {  
    SERVER1 172.168.1.70  
    SERVER2 172.168.1.57  
}
```

Note that the ini option ‘DontCreateConf = 1’ should be set on both servers.

14. Integrations

14.1 KEESING

KEESING is a paid service allowing to check via Internet the authenticity of ID cards, driving licences and passports against the most up to date information from around the world. The KEESING database gives access to over 20.000 images of over 2300 issued documents from 198 countries. Once subscribed to KEESING, it is possible to automatically import data from the Identity Document pictures to the Amadeus 5 cardholder information fields (e.g. First name, Last name, ID number, Photo, Valid to etc).

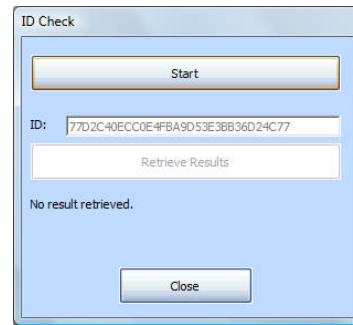


When the ID is tabled on a dedicated passport/ID scanner near the workstation, clicking on the new ‘**ID Check**’ button at the top right of the Amadeus 5 Cardholder screen opens the “ID Check” screen that allows to start the online enrollment wizard from KEESING (for more details see <http://www.keesingreferencesystems.com>).



When the Keesing Intake Wizard is completed and the authentication of the document is finished, pressing “**Retrieve Results**” automatically fills the relevant data in the Cardholder screen and links the scanned ID to the cardholder in the Attached document tab. The user should then ‘Save’ and allocate a card to the cardholder and the appropriated Access group(s) in order it will pass through doors.

To use this integration, the following ini entries should be set first:



KeesingIntegration = 1

KeesingTest [=1 for connection to Test server / =0 for connection to Production server]

KeesingAccount = [Keesing Account name]

KeesingUser = [Keesing User name]

ScannerType = [0- Standard; 1- ARH PRM; 2- ARH_PRMc; 3- 3M/RTE 8000]

14.2 Updated XML-API

In addition to the ‘**AddException**’ function, the XML-API has been updated with the “**DeleteException**” function that allows to delete existing Exceptions from cardholders. In addition, the XML-API has been updated with the two new parameters **<SyncID>** and **<AnswerID>** for being capable to return a response to confirm that Amadeus 5 server has received the command for adding/removing an exception.

14.3 Updated OPC server

Due to the fact OPC is based on polling mode, if Amadeus 5 quickly changes OPC tag value, the OPC client can miss the corresponding event. In order to be sure that the OPC client receives every event, new INI entry ‘**OPCConfirmEventReception = 1**’ allows Amadeus 5 server to wait for OPC client confirmation. Then, only when the OPC client has confirmed the event reception by setting the new tag ‘**DDS_EVENTS RECEIVED**’ to 1, Amadeus 5 can send the next event and immediately reset the tag value to 0. Events that are waiting to be sent to OPC client are stored in the new ‘**OPCEvents.xml**’ file.

15. Communication

15.1 Support for communication with controllers over Internet

Many PCs/Routers do not respond to PING commands and prevent communication between controllers and Amadeus 5 over networks managed by such Routers. A new ini entry ‘**woPing=1**’ allows to avoid the ‘PING’ commands use and then enables Amadeus 5 to communicate with controllers over Internet.

15.2 Controller communication has been optimized

- Improved handling of Controller Buffers**

A new way to preserve the controller buffers has been implemented against loss of data due to a server crash or due to a restart operation during event uploading. The principle consists in placing within files all events waiting to be processed by Amadeus 5.

To enable this function, two new ini file entries are provided:

isPollingToFile = 1 for writing all new records into a buffer file into the folder ‘**\polEvt**’
doSavePollingFiles = 1 for saving the files after treatment into the folder ‘**\polEvt\Done**’ in separate folders per day and per hour (if =0, the files are deleted after treatment).

- **Improved Controller Initialization**

A new optimization has been added to reduce by half the download time to the controllers during complete initialization. It consists of reducing the length of messages sent to controllers for people who own the same settings such as access group, PIN code, crisis level, APB, etc.

There is nothing to do; Amadeus 5 automatically applies this optimization to controllers having Eprom version from **15/10/2010** (or 15/10/2009 for Mega controllers) or later.

Note, when using the INI entry '**Com_DownloadEmployeeDuringProcessing=1**', this feature is not available.

In addition, the preparation of messages to send was improved by using a new Stored Procedure (spAllCardsOfCtl) in the database allowing to save even more time during a complete initialization.

- **Improved Cardholder Download**

Assume a 10-floor building has 10 controllers per floor, making a total of 100 controllers. When a visitor comes at the reception desk to get his new badge, Amadeus 5 server downloads the card to the 100 controllers in a random order, so that access at the ground floor entrance gate may take some time if many visitors arrive at the same time. New improvement enables to assign to each controller a priority order, so that the card is downloaded at the ground floor entrance gate first. New INI option '**sendCtlWithPriority=1**' and new field (sendPriority) in the Controller table in the database have been introduced to set up a priority order in the controllers download. For each controller, the new field should be set with a priority number (0 - 9999). The higher is the number, the greater is the priority.

Note that special priority number '9999' is reserved for adding a second queue of download. In this case, the commands are sent alternatively to controllers having '9999' as priority number and to the other controllers from the regular queue.

For advanced users, two other INI options have been added:

sendMaxCrdHcommandsPriorityAtOnce = 1, to send more than one command in '9999' queue, at each timer (up to 3, default is 1).

sendMaxCrdHcommandsRegularAtOnce = 1, to send more than one command in regular queue, at each timer (up to 3, default is 1).

As this feature needs a database modification, please contact us for details.

- **Improved Access group Download**

New INI option '**UseAGoptimization**' enables to prevent download to controllers any changes on Access Group if no cardholder belongs to this Access Group.

- **Improved Pending command Download**

When huge quantity of pending commands should be sent, the application can run slowly. To avoid such behavior, the number of sent commands has been reduced to 80 per batch. In addition, the default value of the INI option '**Resend Pending**' has been changed to 5, so that every 5min, no more than 80 commands are sent.

16. Tools

16.1 New DDS Maintenance tool for SQL databases

Amadeus 5 SQL database needs continuous maintenance to keep it stable and in good performance shape. DDS developed this easy one-screen tool to allow users define the required maintenance jobs. Using this tool, the user can set his/her preferences for the frequency and the time of day each job should be performed. It also gives the possibility to define email settings so that upon success or failure of each job a corresponding message is sent to the defined email address. The email messages are designed to be very short in order to allow using Mail-To-SMS services and forward them within one standard SMS text message.

All these jobs are saved in the SQL Server and performed by the SQL Agent. Therefore they run regardless of whether Amadeus 5 is running at that time or not.

Note that SQL Express (the free MS-SQL Server) does not include SQL Agent so this tool cannot be set when using SQL Express.

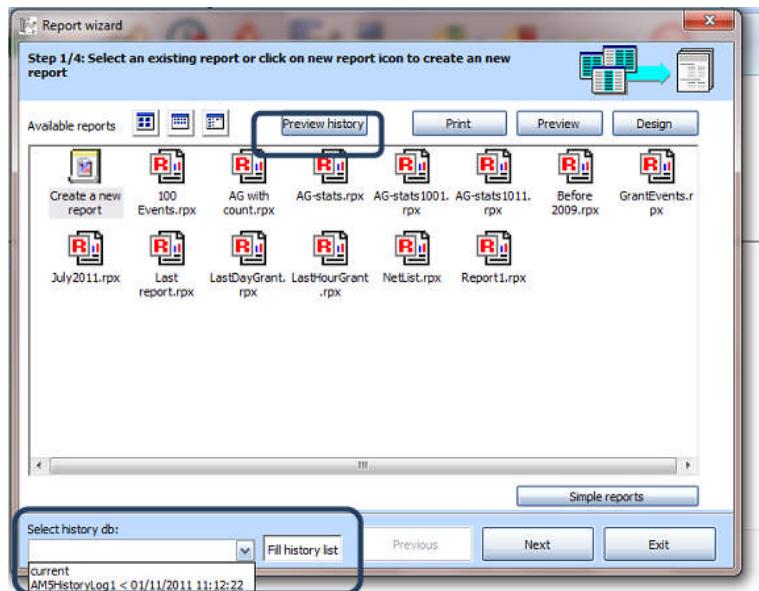


16.2 Log Archiving Support

An option in the DDS Maintenance tool enables to archive old events automatically. These events are removed from the event log table of the main database ([LOGt]) and placed in new external databases. Each archive database contains only one table [LOG], structured exactly like the [LOGt] table in the main database.

When running the Report Wizard, Amadeus 5 detects whether there are archive databases on the SQL Server. If such archives are found, the Wizard displays two new buttons: 'Fill History List' and 'Preview History'. Using these buttons the user can select which one of the history databases should be added to the main database when previewing a pre-defined report.

Note: The Preview History option works only on pre-defined report layouts.



16.3 New DDS tool for converting database from MDB to SQL

New tool has been developed for migrating Amadeus 5 databases from MS-Access to MS-SQL. Please contact us for details.

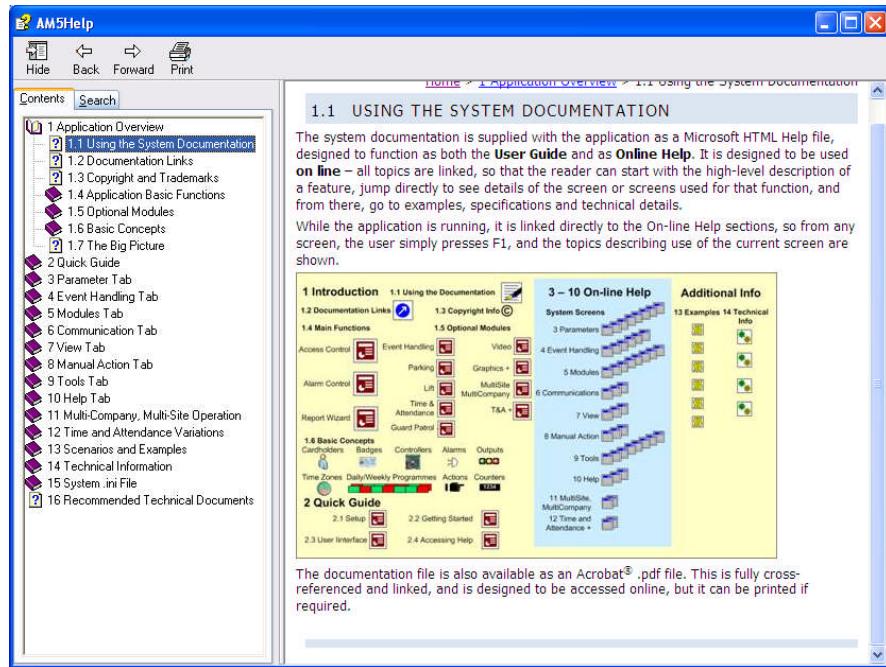
16.4 Automatic tool for deleting old visitors

In some sites, visitors' data are not deleted in Amadeus 5 systematically when visitors left the site, even if visitors left the site many months ago. Then, after some time, the size of the main database has grown significantly. Or, in some countries, legislation requires that personal data of people must be deleted after a certain period of time. Therefore, cleaning the database may be required.

Suppose we want to remove from the database all visitors whose last visit was more than 3 months. New external tool 'EVCleaner' enables to permanently delete from the Amadeus 5 database invalidated cardholders or just visitors that have left the site after a certain period of time. This application detects automatically the database location and includes 'ini' file to define from when the cardholders must be deleted (configurable in months). This tool may be run automatically by Amadeus 5 global reflexes or by Windows scheduler. In addition, it may overwrite every day the event log journal for always having a three months log of events. Please contact us for details.

17. New Help & New Amadeus 5 User Manual

The Amadeus 5 on-line help, opened directly from any Amadeus 5 screen by the F1 key, has been updated in English. As before, this help is screen sensitive, meaning when the F1 is typed from any Amadeus 5 screen the relevant Help page will be shown.



The new help file is automatically installed during the software update or during a new application software setup.

In addition, we have also updated the complete Amadeus 5 User Manual (located on the setup CD), which contains the same information in PDF format. The User Manual file can be downloaded at: www.dds-security.com/download/am5/manual/am5manual.pdf

18. Additional Language

Translations for Italian language have been added.

19. MS/SQL2008

Amadeus 5 is compatible with MS/SQL2008 databases including Express licenses.